



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/980,271	11/30/2001	Alain Delpuch	5266-09100	1037
44015	7590	09/07/2007	EXAMINER	
OPTV/MEYERTONS				BROWN, RUEBEN M
RORY D. RANKIN				
P.O. BOX 398				
AUSTIN, TX 78767-0398				
ART UNIT		PAPER NUMBER		
		2623		
MAIL DATE			DELIVERY MODE	
09/07/2007			PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/980,271
Filing Date: November 30, 2001
Appellant(s): DELPUCH, ALAIN

MAILED
SEP 07 2007
Technology Center 2600

Rory D. Rankin
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 05/07/2007 appealing from the Office action mailed 4/20/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,338,138	RADUCHEL, et al	1-2002
6,122,741	PATTERSON, et al	9-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raduchel, (U.S. Pat # 6,338,138) in view of Patterson, (U.S. pat # 6,122,741).

Considering amended claim 1, the claimed system for authenticating a PIN code of a user in an interactive information system in order to run an application, comprising;

‘an input device for PIN entry’, is met by the input device 110 of Raduchel, col. 3, lines 55-60 & Fig. 1.

‘security manager configured to: receive a request for user authentication from the application’ is met by the disclosure in Raduchel that when a user attempts to access certain

services using a browser (such as icons 502-506), to which the instant user is not already authenticated, the browser sends request to an authentication manger 128, to authenticate the instant user, see col. 5, lines 50-65. Thus, the claimed ‘application’ is broad enough to read on the browser or any of the services that the user seeks to access.

‘compare a received PIN code of user with a registered PIN code, in response to the request is met by the operation of the authentication manager 128, in conjunction with the authentication file 130, col. 3, lines 25-40 & col. 4, lines 9-25.

‘supply information to the application about PIN code entering key-pressing operations by the user, wherein the PIN code is not supplied to the application’ and ‘wherein the application is configured to present a PIN entry field, such that the cryptd information corresponding to the information about the PIN code is displayed in the PIN entry field’, in Raduchel, when the user enters the log-in information, it is delivered directly to the authentication manager 128, which reads on the claimed subject matter, col. 5, lines 17-35. However Raduchel does not disclose that the user is presented with the PIN being hidden or cryptd. Nevertheless Patterson, which is in the same field of endeavor discloses blocking from display the actual characters entered by the user, see Fig. 5. It would have been obvious for one of ordinary skill in the art at the time the invention was made to not allow the passwords to be shown, as disclosed by Patterson, for the desirable improvement of keeping the subscriber’s password confidential even if another person is in the room and observes the password being entered.

'give authorization to run the application if the PIN code of the user matches the registered PIN code', is also met by the operation of the authentication manager 128., see col. 3, lines 30-45.

Considering claims 2-3, 7-8 & 10-11, even though Raduchel does not disclose its use with a TV or mobile phone system, Official Notice is taken that the time the invention was made, it was well known in the art to use PIN or password security in a TV or mobile phone system. It would have been obvious for one of ordinary skill in the art at the time the invention was made to use a PIN or password feature in a TV or mobile phone system, at least for the desirable purpose of prohibiting unauthorized use of programming on those devices.

Considering claim 4, the claimed method for authenticating a PIN code of a user, comprising elements that correspond with subject matter mentioned above in the rejection of claim 1, are likewise treated.

Considering claim 9, the claimed computer readable medium comprising executable instructions for authenticating a PIN code of a user, comprising elements that correspond with subject matter mentioned above in the rejection of claim 1, are likewise treated.

(10) Response to Argument

In the Summary of the Claimed Subject Matter, on page 6, Appellant states, “The security manager is configured to receive a request for user authentication from the application; compare a received PIN code of the user with a registered PIN code, in response to the request; supply information to the application about the PIN code entering key-pressing operation by the user, wherein the entered PIN code is not supplied to the application”, emphasis added.

Examiner notes that the password discussed in Raduchel, corresponds with the PIN as claimed.

Furthermore, in the introduction to Arguments, on page 9 of the Brief, Appellant discusses that “two types of solutions are known for authentication in the prior art”. “In a first case, the application presents its own user interface for PIN entry, receives input, and queries the underlying system to check if the PIN is correct. However, this solution does not hide the PIN code from the application”, emphasis added.

First of all, it is noted that while the claims do recite that, ‘crypted information corresponding to PIN code entering key-pressing operations are received from the security’, this step is at the back-end of the authentication process. The front-end of the authentication process is the claimed, ‘security manager configured to receive a request for user authentication from the application’. However, the claims do not explicitly point out where in the system the ‘security

manager' operates. This is important, because the claims as written are broad enough to read on the security manger operating at the server or database.

Secondly, it is noted that the claims do not recite any entity that receives the PIN (on the front end), i.e., directly from the input device and delivers the PIN to the claimed 'security manager'. Thus the claims are broad enough to read on the security manger receiving the PIN code from some other entity, (including an intermediary or the application itself) and then comparing the received PIN code, with the stored value, as recited.

Even though Appellant has argued throughout that PIN code is hidden from the application, there is no language recited in claims that support such a requirement.

In light the above analysis of the recited limitations, examiner asserts that Appellant's argument on page 13, that it is the browser in Raduchel that presents the dialog box, instead of the application, is a moot point.

Moreover, since the application is operated or accessed in conjunction with the browser, the browser reads on the application. Since the user is essentially requesting to use the browser in a certain manner, i.e., in conjunction with the requested application, the browser does read on the application, in a broad sense

Appellant argues on page 13 that the browser in Raduchel is separate from the application that user desires authentication for, and since it is the browser that presents the dialog box, instead of the application, Raduchel does not meet the claim. Examiner notes that Raduchel more specifically teaches that the first time that the user selects an icon corresponding to a particular application that the browser sends a request to the authentication manager, which then sends the appropriate applet that will display the logon screen, col. 3, lines 5-28 & col. 5, lines 5-8. Subsequently, the applet is already stored at the PC and is called on by the browser, when the user again requests to be authenticated to the particular application, col. 5, lines 50-62.

Thus, the claims as written are broad enough to read on the applet that is downloaded from the remote source and is associated with a particular application or group of applications. The ‘application configured to present the PIN entry field’, would then read on the applet presenting the dialog box, as disclosed Raduchel, since again in the applet is associated with a particular application.

Col. 3, lines 30-35 discloses that in fact the authentication manger in Raduchel does receive the password (e.g., PIN) and determines whether the values are valid, as recited in the claims.

As for the additional feature of the security manager supplying the crypted for display, first of all Patterson teaches that it is the client application that displays the logon dialog box, which corresponds with the claimed subject matter, col. 3, lines 45-51. Patterson meets the

claimed subject matter, since the security administration client 17 (which reads on the claimed ‘security manager’) is the entity that receives the logon information and interfaces with the client workstation. Fig. 5 shows that the password/PIN information is displayed on the screen in a encrypted form, as recited in the claims. Thus, the claimed feature is met by the combination of Raduchel & Patterson.

In the Final Rejection, with respect to claims 2-3 & 7-8, examiner took Official Notice that at the time the invention was made, it was well known in the art to use PIN or password security in a TV or mobile phone system. In support of the Official Notice, Urakoshi (U.S. Pat # 6,067,564), col. 4, lines 25-41 is cited for claims 2, 7 & 10. The reference teaches that passwords are used to gain to various services, whereas the actual password is not shown on the screen.

Shin (U.S. Pat # 6,351,634) is cited for claims 3, 8 & 11, which is directed to using the touch screen of a mobile telephone to enter a password: Abstract; col. Fig. 1; col. 5, lines 31-51; col. 7, lines 51-67 thru col. 8, lines 1-15.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Reuben M. Brown


REUBEN M. BROWN
PATENT EXAMINER

Conferees:

Christopher Kelly

Vivek Srisivatsava


CHRIS KELLEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600


VIVEK SRIVASTAVA
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600